

# Hlášení kybernetických bezpečnostních incidentů



**Incident** je narušení bezpečnosti informací v rámci aktiv.

**Bezpečnost informací** je zajištění důvěrnosti, integrity a dostupnosti informací a dat.



Účinnost zákona se předpokládá k 1. lednu 2025.

Poskytovatelé regulovaných služeb hlásí kybernetické bezpečnostní incidenty **nejpozději do 1 roku** po doručení rozhodnutí o registraci.

## CO A KOMU HLÁSIT?

### Povinná osoba ve vyšším režimu

Všechny incidenty, které

- mají původ v kybernetickém prostoru **a zároveň**
- nelze u nich vyloučit úmyslné zavinění.

Incidenty se hlásí NÚKIB.

### Povinná osoba v nižším režimu

Všechny incidenty, které

- mají původ v kybernetickém prostoru,
- mají významný dopad (způsob stanovení ve vyhlášce) **a zároveň**
- nelze u nich vyloučit úmyslné zavinění.

Incidenty se hlásí Národnímu CERT.

## KDY A CO PŘESNĚ HLÁSIT?

### Prvotní hlášení

**KDY:** Bez zbytečného odkladu po zjištění incidentu, nejpozději do 24 hodin.

**CO:** Identifikační údaje organizace, základní údaje o incidentu, zda byl incident způsoben nezákonným zásahem, zda by incident mohl mít přeshraniční dopad.

### Oznámení

**KDY:** Bez zbytečného odkladu, nejpozději do 72 hodin (poskytovatel služeb vytvářejících důvěru do 24 hodin) po zjištění incidentu aktualizace informací z prvotního hlášení.

**CO:** Prvotní posouzení incidentu, dopad incidentu, indikátory kompromitace.

### Průběžná zpráva

**KDY:** Na výzvu NÚKIB nebo Národního CERT.

**CO:** Průběžná zpráva o podstatných změnách stavu zvládání incidentu.

NÚKIB poskytovateli regulované služby ve vyšším režimu po prvotním hlášení oznámí, zda má incident významný dopad. **Pokud je incident bez významného dopadu, tímto krokem hlášení pro organizaci končí.**

Pokud incident stále trvá, předloží organizace po uplynutí lhůty **průběžnou zprávu o aktuálním stavu zvládání incidentu**, a po jeho vyřešení nejpozději do 30 dnů závěrečnou zprávu o vyřešení incidentu.

### Závěrečná zpráva

**KDY:** Nejpozději do 30 dnů od oznámení.

**CO:** Podrobný popis incidentu, jeho závažnosti a dopadu, druh hrozby, pravděpodobnou příčinu incidentu, učiněná a probíhající opatření ke zmírnění následků a případný přeshraniční dopad incidentu.